



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0129685
(43) 공개일자 2023년09월11일

(51) 국제특허분류(Int. Cl.)

G09B 19/00 (2006.01) G06F 21/57 (2013.01)
G09B 23/18 (2006.01) G09B 7/02 (2006.01)
H04L 67/12 (2022.01) H04L 9/40 (2022.01)

(52) CPC특허분류

G09B 19/0053 (2013.01)
G06F 21/577 (2013.01)

(21) 출원번호 10-2022-0026592

(22) 출원일자 2022년03월02일
심사청구일자 2022년03월02일

(71) 출원인

건양대학교산학협력단
충청남도 논산시 대학로 121 (내동)

(72) 발명자

김동원
충청남도 논산시 연무읍 안심로 150-22 골든팰리스 102동 1602호

(74) 대리인

강정빈, 심찬, 송두현

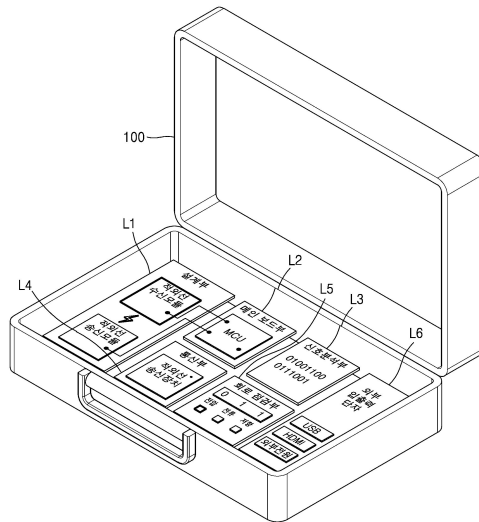
전체 청구항 수 : 총 5 항

(54) 발명의 명칭 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법

(57) 요약

본 발명은 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법의 제공 방법으로서, 학습자가 적외선통신 모의해킹 실습장치를 통해 적외선헤킹모듈을 구성해보고, 해당 모듈에 대한 소스코드를 작성하는 방식으로 적외선통신 모의해킹을 실습하게 하고, 학습자의 실습결과에 대한 스코어를 산출하여 제공하는, 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법에 관한 것이다.

대표도 - 도1



(52) CPC특허분류

G09B 23/186 (2013.01)

G09B 7/02 (2013.01)

H04L 63/1441 (2013.01)

H04L 67/12 (2022.05)

명세서

청구범위

청구항 1

적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법으로서,

상기 적외선통신 모의해킹 실습장치는,

브레드보드로 구성되고, 적외선송신센서, 적외선수신센서, 전원, 저항, 증폭기, 및 LED를 포함하는 전자부품을 사용하여 적외선수신모듈 및 적외선송신모듈을 구성하고 이에 대한 전기회로를 설계할 수 있는 설계부;

1 이상의 프로세서 및 1 이상의 메모리를 포함하는 마이크로컨트롤러를 포함하고, 외부 컴퓨팅장치로부터 수신한 소스코드에 기초하여 상기 설계부에 설계된 적외선수신모듈 및 적외선송신모듈의 동작을 제어하는 메인보드부;

USB포트, HDMI 포트 및 외부전원소켓에 의해 외부 컴퓨팅장치와 연결되어, 상기 외부 컴퓨팅장치에서 작성된 적외선수신모듈 및 적외선송신모듈에 대한 소스코드를 수신하는, 외부입출력단자;

상기 설계부에 설계된 적외선수신모듈 및 적외선송신모듈에 대한 전기회로의 단선 여부 및 전압, 전류, 저항을 측정하여, 상기 적외선수신모듈 및 적외선송신모듈이 올바르게 구성되었는지 여부를 점검하는 회로점검부;

상기 메인보드부에 의해 적외선통신을 수행하는 적외선수신모듈 및 적외선송신모듈간에 송수신되는 데이터 패킷을 디스플레이하는 신호분석부; 및

상기 메인보드부에 의해 생성된 명령에 따라 적외선 신호를 생성하여 모의해킹 대상장치에 송신하는, 통신부;를 포함하고,

상기 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법은,

상기 설계부상에서 학습자가 실습하고자 하는 모의해킹 사례에 따라 적외선수신모듈 및 적외선송신모듈을 구성 및 이에 대한 전기회로를 설계하고, 상기 외부입출력단자에 의해 연결된 상기 외부 컴퓨팅장치에서 상기 적외선수신모듈 및 적외선송신모듈에 대한 소스코드를 작성하여 적외선통신 모의해킹을 실습하는, 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법.

청구항 2

청구항 1에 있어서,

상기 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법은,

상기 학습자가 적외선통신 모의해킹을 수행함에 따른 출력결과에 기초하여, 상기 학습자가 작성한 소스코드가 유효한지 여부 및 모의해킹 대상장치의 보안취약점을 분석하는 단계를 더 포함하는, 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법.

청구항 3

청구항 1에 있어서,

상기 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법은,

적외선수신모듈이 공격수행모듈이 되어 적외선수신모듈 및 적외선수신모듈간에 송수신되는 데이터 패킷을 스니핑하는 스니핑시나리오; 및

적외선송신모듈이 공격수행모듈이 되어 적외선수신모듈 및 적외선수신모듈간에 송수신되는 데이터 패킷을 위변조하는 위변조시나리오;에 대한 적외선통신 공격사례를 모의로 실험할 수 있는, 적외선통신 모의해킹 실습장치

를 활용하여 수행되는 IoT보안교육방법.

청구항 4

청구항 1에 있어서,

상기 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법은,

상기 학습자가 적외선통신 모의해킹을 수행함에 따른 실습결과에 대한 스코어를 산출하는 스코어산출단계;를 더 포함하고,

상기 스코어산출단계는,

상기 회로점검부에 의해 점검된, 상기 학습자가 구성한 적외선수신모듈, 및 적외선송신모듈이 전기회로적으로 올바르게 구성되었는 지 여부에 대한 스코어를 산출하는 제1스코어산출단계;

상기 학습자가 작성한 적외선수신모듈, 및 적외선송신모듈을 동작시키는 소스코드에 대한 디버깅을 수행하여, 상기 소스코드의 유효성에 기초하여 스코어를 산출하는 제2스코어산출단계; 및

상기 학습자가 입력한 상기 소스코드와 모의해킹이 수행됨에 따라 출력된 출력결과를 비교하여, 모의해킹이 정상적으로 수행되는지 여부에 기초하여 스코어를 산출하는 제3스코어산출단계;를 포함하는, 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법.

청구항 5

청구항 4에 있어서,

상기 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법은,

상기 스코어를 기설정된 이하로 기록한 상기 학습자의 컴퓨팅장치에 적외선통신 모의해킹에 대한 답안을 제공하는, 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법.

발명의 설명

기술 분야

[0001] 본 발명은 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법의 제공 방법으로서, 학습자가 적외선통신 모의해킹 실습장치를 통해 적외선통신모듈을 구성해보고, 해당 모듈에 대한 소스코드를 작성하는 방식으로 적외선통신 모의해킹을 실습하게 하고, 학습자의 실습결과에 대한 스코어를 산출하여 제공하는, 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법에 관한 것이다.

배경 기술

[0003] 현대사회에 도래하고 있는 4차 산업혁명에서 사물인터넷(Internet of Things)은 사물과 사물간의 자율적인 소통이 가능하도록 사물 내에 센서 및 통신장치 등을 탑재하여 네트워크에 연결된 다양한 사물들과 데이터를 주고받을 수 있는 기술로써, 다양한 산업을 이끌 수 있는 혁신적인 기술로 여겨지고 있다.

[0004] IoT기술은 자동차, 가전, 헬스케어 등 다양한 분야에서 활용되어 일상생활에서의 각종 편리함을 제공하고 있다. 그러나 이와 같이 IoT기술이 일상생활에서 광범위하게 활용됨에 따라, 사물인터넷에 대한 보안 위협은 기존의 보안위협과 달리 사용자의 신체, 재산에 대한 심각한 피해를 발생시킬 가능성이 있다.

[0005] 일례로 가정에서 사용되는 IP카메라를 해킹하거나 실시간 화상 강의 중인 웹캠을 해킹하여 불법 촬영물을 유포하거나 적외선통신을 사용하는 의료기기를 해킹하여 공격하는 사례가 보고된 바 있다.

[0006] 이에 따라 사물인터넷 환경에서의 해킹공격을 방어할 수 있는 보안전문가를 양성하기 위해서는 소프트웨어 기반

의 지식교육과 함께 하드웨어 기반의 실습교육이 수반될 필요가 있다. 구체적으로 적외선통신 모의해킹은 이러한 교육의 일환으로서, 적외선을 송수신하는 모듈을 구성하고, 해당 모듈에 공격을 수행하는 소스코드를 짜는 방식으로 이루어질 수 있다.

[0007] 그러나 이와 같이 모듈을 구성하는 방식의 교육방식은 교육자가 학습자 개개인별로 실습모듈을 구성하는 전자부품을 준비하고 평가를 수행해야 하므로, 다수의 학습자에 대한 실습교육을 수행하기에 어려운 문제점이 있었다.

[0008] 따라서 상기와 같은 문제를 해결하고자 적외선통신 모의해킹을 실습할 수 있는 장치를 제공하여, 해당 장치를 적외선통신 모의해킹을 실습하고, 실습결과에 대한 평가를 자동으로 수행하여 교육자의 부담을 경감할 수 있는 방법 및 시스템에 대한 개발 필요성이 대두되고 있다.

발명의 내용

해결하려는 과제

[0010] 본 발명은 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법의 제공 방법으로서, 학습자가 적외선통신 모의해킹 실습장치를 통해 적외선헤킹모듈을 구성해보고, 해당 모듈에 대한 소스코드를 작성하는 방식으로 적외선통신 모의해킹을 실습하게 하고, 학습자의 실습결과에 대한 스코어를 산출하여 제공하는, 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0012] 상기와 같은 과제를 해결하기 위하여, 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법으로서, 상기 적외선통신 모의해킹 실습장치는, 브레드보드로 구성되고, 적외선송신센서, 적외선수신센서, 전원, 저항, 증폭기, 및 LED를 포함하는 전자부품을 사용하여 적외선수신모듈 및 적외선송신모듈을 구성하고 이에 대한 전기회로를 설계할 수 있는 설계부; 1 이상의 프로세서 및 1 이상의 메모리를 포함하는 마이크로컨트롤러를 포함하고, 외부 컴퓨팅장치로부터 수신한 소스코드에 기초하여 상기 설계부에 설계된 적외선수신모듈 및 적외선송신모듈의 동작을 제어하는 메인보드부; USB포트, HDMI 포트 및 외부전원소켓에 의해 외부 컴퓨팅장치와 연결되어, 상기 외부 컴퓨팅장치에서 작성된 적외선수신모듈 및 적외선송신모듈에 대한 소스코드를 수신하는, 외부입출력단자; 상기 설계부에 설계된 적외선수신모듈 및 적외선송신모듈에 대한 전기회로의 단선 여부 및 전압, 전류, 저항을 측정하여, 상기 적외선수신모듈 및 적외선송신모듈이 올바르게 구성되었는지 여부를 점검하는 회로점검부; 상기 메인보드부에 의해 적외선통신을 수행하는 적외선수신모듈 및 적외선송신모듈간에 송수신되는 데이터 패킷을 디스플레이하는 신호분석부; 및 상기 메인보드부에 의해 생성된 명령에 따라 적외선 신호를 생성하여 모의해킹 대상장치에 송신하는, 통신부;를 포함하고, 상기 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법은, 상기 설계부상에서 학습자가 실습하고자 하는 모의해킹 사례에 따라 적외선수신모듈 및 적외선송신모듈을 구성 및 이에 대한 전기회로를 설계하고, 상기 외부입출력단자에 의해 연결된 상기 외부 컴퓨팅장치에서 상기 적외선수신모듈 및 적외선송신모듈에 대한 소스코드를 작성하여 적외선통신 모의해킹을 실습하는, 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법을 제공한다.

[0013] 본 발명의 일 실시예에서는 상기 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법은, 상기 학습자가 적외선통신 모의해킹을 수행함에 따른 출력결과에 기초하여, 상기 학습자가 작성한 소스코드가 유효한지 여부 및 모의해킹 대상장치의 보안취약점을 분석하는 단계를 더 포함할 수 있다.

[0014] 본 발명의 일 실시예에서는 상기 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법은, 적외선수신모듈이 공격수행모듈이 되어 적외선수신모듈 및 적외선수신모듈간에 송수신되는 데이터 패킷을 스니핑하는 스니핑시나리오; 및 적외선송신모듈이 공격수행모듈이 되어 적외선수신모듈 및 적외선수신모듈간에 송수신되는 데이터 패킷을 위변조하는 위변조시나리오;에 대한 적외선통신 공격사례를 모의로 실습할 수 있다.

[0015] 본 발명의 일 실시예에서는 상기 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법은, 상기 학습자가 적외선통신 모의해킹을 수행함에 따른 실습결과에 대한 스코어를 산출하는 스코어산출단계;를 더 포함하고, 상기 스코어산출단계는, 상기 회로점검부에 의해 점검된, 상기 학습자가 구성한 적외선수신모듈, 및 적외선송신모듈이 전기회로적으로 올바르게 구성되었는지 여부에 대한 스코어를 산출하는 제1스코어산출단계; 상기 학습자가 작성한 적외선수신모듈, 및 적외선송신모듈을 동작시키는 소스코드에 대한 디버깅을 수행하여, 상기

소스코드의 유효성에 기초하여 스코어를 산출하는 제2스코어산출단계; 및 상기 학습자가 입력한 상기 소스코드와 모의해킹이 수행됨에 따라 출력된 출력결과를 비교하여, 모의해킹이 정상적으로 수행되는지 여부에 기초하여 스코어를 산출하는 제3스코어산출단계;를 포함할 수 있다.

[0016] 본 발명의 일 실시예에서는 상기 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법은, 상기 스코어를 기설정된 이하로 기록한 상기 학습자의 컴퓨팅장치에 적외선통신 모의해킹에 대한 답안을 제공할 수 있다.

발명의 효과

[0018] 본 발명의 일 실시예에 따르면 학습자는 적외선통신 공격유형에 대한 복수의 공격시나리오 중 실습하고자 하는 공격시나리오를 선택하여, 적외선통신 모의해킹을 실습할 수 있다.

[0019] 본 발명의 일 실시예에 따르면 학습자는 적외선통신 모의해킹을 수행하는 적외선헤킹모듈을 디자인하고 전기회로를 구성해보는 방식으로 적외선통신 모의해킹을 실습할 수 있다.

[0020] 본 발명의 일 실시예에 따르면 학습자는 적외선통신 모의해킹을 수행하는 적외선헤킹모듈에 대한 소스코드를 작성하는 방식으로 적외선통신 모의해킹을 실습할 수 있다.

[0021] 본 발명의 일 실시예에 따르면 학습자가 구성한 적외선헤킹모듈이 적외선통신 모의해킹을 수행한데 따른 출력결과를 제공할 수 있다.

[0022] 본 발명의 일 실시예에 따르면 학습자가 구성한 적외선통신 모의해킹 수행과정 및 수행결과에 따른 스코어를 산출하여 제공할 수 있다.

[0023] 본 발명의 일 실시예에 따르면 다수의 학습자를 관리감독하는 교육자에게 학습자 개개인의 실습진행정보 및 스코어를 제공할 수 있다.

도면의 간단한 설명

[0025] 도 1은 본 발명의 일 실시예에 따른 적외선통신 모의해킹 실습장치를 도시한 것이다.

도 2는 본 발명의 일 실시예에 따른 외부 컴퓨팅장치에 의해 적외선통신 모의해킹 실습장치에 소스코드를 입력하는 단계를 도시한 것이다.

도 3은 본 발명의 일 실시예에 따른 통신부에 의해 모의해킹 대상장치에 적외선 신호를 송신하는 단계를 도시한 것이다.

도 4는 본 발명의 일 실시예에 따른 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법의 수행단계를 도시한 것이다.

도 5는 본 발명의 일 실시예에 따른 적외선수신모듈 및 적외선송신모듈에 적외선통신 모의해킹을 수행하는 소스코드를 입력하고, 모의해킹 수행결과에 기초하여 모의해킹 대상장치에 대한 분석을 수행하는 단계를 도시한 것이다.

도 6은 본 발명의 일 실시예에 따른 학습자가 모의해킹을 수행함에 따른 스코어를 산출하는 단계를 도시한 것이다.

도 7은 본 발명의 일 실시예에 따른 교육자단말 및 1 이상의 학습자단말에 의해 IoT보안교육이 실시되는 일 모습을 도시한 것이다.

발명을 실시하기 위한 구체적인 내용

[0026] 이하에서는, 다양한 실시예들 및/또는 양상들이 이제 도면들을 참조하여 개시된다. 하기 설명에서는 설명을 목적으로, 하나이상의 양상들의 전반적 이해를 돕기 위해 다수의 구체적인 세부사항들이 개시된다. 그러나, 이러한 양상(들)은 이러한 구체적인 세부사항들 없이도 실행될 수 있다는 점 또한 본 발명의 기술 분야에서 통상의 지식을 가진 자에게 인식될 수 있을 것이다. 이후의 기재 및 첨부된 도면들은 하나 이상의 양상들의 특정한 예

시적인 양상들을 상세하게 기술한다. 하지만, 이러한 양상들은 예시적인 것이고 다양한 양상들의 원리들에서의 다양한 방법들 중 일부가 이용될 수 있으며, 기술되는 설명들은 그러한 양상들 및 그들의 균등물들을 모두 포함하고자 하는 의도이다.

- [0028] 또한, 다양한 양상들 및 특징들이 다수의 디바이스들, 컴포넌트들 및/또는 모듈들 등을 포함할 수 있는 시스템에 의하여 제시될 것이다. 다양한 시스템들이, 추가적인 장치들, 컴포넌트들 및/또는 모듈들 등을 포함할 수 있다는 점 그리고/또는 도면들과 관련하여 논의된 장치들, 컴포넌트들, 모듈들 등 전부를 포함하지 않을 수도 있다는 점 또한 이해되고 인식되어야 한다.
- [0029] 본 명세서에서 사용되는 "실시예", "예", "양상", "예시" 등은 기술되는 임의의 양상 또는 설계가 다른 양상 또는 설계들보다 양호하다거나, 이점이 있는 것으로 해석되지 않을 수도 있다. 아래에서 사용되는 용어들 '~부', '컴포넌트', '모듈', '시스템', '교육인터페이스' 등은 일반적으로 컴퓨터 관련 엔티티(computer-related entity)를 의미하며, 예를 들어, 하드웨어, 하드웨어와 소프트웨어의 조합, 소프트웨어를 의미할 수 있다.
- [0030] 또한, "포함한다" 및/또는 "포함하는"이라는 용어는, 해당 특징 및/또는 구성요소가 존재함을 의미하지만, 하나 이상의 다른 특징, 구성요소 및/또는 이들의 그룹의 존재 또는 추가를 배제하지 않는 것으로 이해되어야 한다.
- [0031] 또한, 제1, 제2 등과 같이 서수를 포함하는 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되지는 않는다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.
- [0032] 또한, 본 발명의 실시예들에서, 별도로 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 발명의 실시예에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.
- [0034] 본 발명에 대한 상세한 설명에 앞서, 본원 발명에서 제공하는 적외선통신 모의해킹 실습장치를 활용하여 수행되는 IoT보안교육방법은 학습자로 하여금 적외선통신 모의해킹의 다양한 사례에 대해 하드웨어 및 소프트웨어적으로 실습할 수 있는 교육환경을 제공하는 것을 목적으로 한다.
- [0035] 본원 발명에서는 적외선통신 모의해킹의 다양한 사례에 대한 공격시나리오를 구성하여 학습자에게 제공할 수 있다.
- [0036] 구체적으로 공격시나리오는 적외선을 쏘아서 정보를 송수신하는 적외선 통신기술을 공격하는 공격유형에 대한 시나리오로서, 데이터 스푸핑(Spoofing), 스니핑(Sniffing), 스누핑(Snooping), 및 데이터 위변조와 같은 공격유형과 스마트폰, TV, 리모컨, 디지털카메라와 같은 적외선 통신 적용사례에 따라 생성될 수 있다.
- [0037] 바람직하게는 공격시나리오는 TV-리모컨간에 송수신되는 데이터 패킷을 해킹하여 TV의 음량을 조절하거나 ON-OFF하는 공격사례 또는 적외선송수신모듈간에 송수신되는 데이터 패킷을 위변조하거나 탈취하는 공격사례를 실습할 수 있게 재현된 시나리오이다.
- [0039] 학습자는 상기와 같이 제공되는 복수의 공격시나리오 중 실습하고자 하는 공격시나리오를 선택하여 적외선통신 모의해킹 실습을 시작할 수 있다.
- [0041] 도 1은 본 발명의 일 실시예에 따른 적외선통신 모의해킹 실습장치(100)를 도시한 것이다.
- [0043] 도 1에 도시된 바와 같이, 적외선통신 모의해킹 실습장치(100)를 활용하여 수행되는 IoT보안교육방법으로서, 상기 적외선통신 모의해킹 실습장치(100)는, 브레드보드로 구성되고, 적외선송신센서, 적외선수신센서, 전원, 저

항, 증폭기, 및 LED를 포함하는 전자부품을 사용하여 적외선수신모듈 및 적외선송신모듈을 구성하고 이에 대한 전기회로를 설계할 수 있는 설계부(L1); 1 이상의 프로세서 및 1 이상의 메모리를 포함하는 마이크로컨트롤러를 포함하고, 외부 컴퓨팅장치(200)로부터 수신한 소스코드에 기초하여 상기 설계부(L1)에 설계된 적외선수신모듈 및 적외선송신모듈의 동작을 제어하는 메인보드부(L2); USB포트, HDMI 포트 및 외부전원소켓에 의해 외부 컴퓨팅장치(200)와 연결되어, 상기 외부 컴퓨팅장치(200)에서 작성된 적외선수신모듈 및 적외선송신모듈에 대한 소스코드를 수신하는, 외부입출력단자(L6); 상기 설계부(L1)에 설계된 적외선수신모듈 및 적외선송신모듈에 대한 전기회로의 단선 여부 및 전압, 전류, 저항을 측정하여, 상기 적외선수신모듈 및 적외선송신모듈이 올바르게 구성되었는 지 여부를 점검하는 회로점검부(L5); 상기 메인보드부(L2)에 의해 적외선통신을 수행하는 적외선수신모듈 및 적외선송신모듈간에 송수신되는 데이터 패킷을 디스플레이하는 신호분석부(L3); 및 상기 메인보드부(L2)에 의해 생성된 명령에 따라 적외선 신호를 생성하여 모의해킹 대상장치에 송신하는, 통신부(L4);를 포함할 수 있다.

[0045] 설계부(L1)는 학습자가 적외선통신 모의해킹을 수행하는 적외선수신모듈 및 적외선송신모듈을 하드웨어적으로 구성해볼 수 있는 구성요소이다. 구체적으로 상기 설계부(L1)는 브레드보드로 구성되고 학습자는 적외선송신센서, 적외선수신센서, 전원, 저항, 증폭기, 및 LED와 같은 전자부품을 사용하여 적외선수신모듈 및 적외선송신모듈을 구성하고, 이에 대한 전기회로를 설계할 수 있다.

[0046] 또한 학습자에 의해 설계된 적외선수신모듈 및 적외선송신모듈은 메인보드부(L2)와 전기적으로 연결되어, 메인보드부(L2)에 의해 상기 적외선수신모듈 및 적외선송신모듈의 동작을 제어하도록 할 수 있다.

[0047] 학습자가 설계부(L1)에서 구성하는 적외선수신모듈 및 적외선송신모듈의 형태는 학습자가 수행하는 공격시나리오 따라 상이할 수 있다.

[0048] 일례로, 학습자가 실습하고자 하는 공격시나리오가 '스니핑 시나리오'에 해당하는 경우, 학습자는 설계부(L1)의 브레드보드상에서 적외선송신센서, 적외선수신센서, 전원, 저항, 증폭기, 및 LED를 이용해 적외선송신모듈 및 적외선수신모듈을 구성하고, 상기 모듈들과 메인보드부(L2)를 전기적으로 연결하는 방식으로 하드웨어적 실습교육을 수행할 수 있다.

[0050] 또는, 학습자가 실습하고자 하는 공격시나리오가 'TV-리모콘간에 송수신되는 데이터 패킷을 해킹'하는 것에 해당하는 경우, 적외선수신모듈에 해당하는 장치는 외부장치인 TV가 될 수 있고, 해당 경우에 학습자는 리모콘에 대응하는 적외선송신모듈을 구성하고, 상기 적외선송신모듈과 메인보드부(L2)를 전기적으로 연결하는 방식의 실습교육을 수행할 수 있다.

[0051] 한편, 상기와 같은 경우에 메인보드부(L2)는 적외선송신모듈이 생성하는 적외선 신호와 동일한 신호를 통신부(L4)가 생성하게 하여, 모의해킹 대상장치인 TV로 송신하게 할 수 있다.

[0053] 메인보드부(L2)는 1 이상의 프로세서 및 1 이상의 메모리를 포함하는 마이크로컨트롤러를 포함하여, 실습장치의 총체적 제어를 담당하는 구성요소로서, 설계부(L1), 외부입출력단자(L6), 회로점검부(L5), 신호분석부(L3), 통신부(L4)와 전기적으로 연결되어 각 구성요소의 동작을 제어할 수 있다.

[0054] 구체적으로 학습자단말이 작성한 소스코드는 외부입출력단자(L6)에 의해 메인보드부(L2)에 입력되어, 메인보드부(L2)가 입력받은 소스코드에 따라 설계부(L1)에 구성된 적외선수신모듈 및 적외선송신모듈을 동작하게 할 수 있다.

[0055] 또한, 메인보드부(L2)는 신호분석부(L3)에 적외선수신모듈 및 적외선송신모듈간의 송수신되는 데이터 패킷을 디스플레이하도록 명령하거나, 통신부(L4)에 적외선신호를 생성하도록 명령하여 TV,스마트폰과 같이 외부에 존재하는 모의해킹 대상장치로 적외선신호를 송신하게 할 수 있다.

[0057] 회로점검부(L5)는 적외선수신모듈 및 적외선송신모듈이 전기적으로 올바르게 구성되었는 지 여부를 점검하는 구성요소로서, 설계부(L1) 및 메인보드부(L2)와 전기적으로 연결되어 메인보드부(L2)에 명령에 의해 설계부(L1)에 구성된 적외선수신모듈 및 적외선송신모듈에 대한 전기회로를 점검할 수 있다.

- [0058] 구체적으로 회로점검부(L5)는 별도의 디스플레이패널을 더 포함하고, 설계부(L1)에 구성된 적외선수신모듈 및 적외선송신모듈에 대한 전기회로의 전압, 전류, 저항 등을 측정하여 상기 디스플레이패널에 디스플레이할 수 있다.
- [0059] 또한, 회로점검부(L5)는 별도의 음성출력장치를 더 포함하여, 적외선송신모듈 및 적외선수신모듈이 하드웨어적으로 올바르게 구성되지 않은 경우로 판별되는 경우에 부저음을 출력하여 학습자가 적외선송신모듈 및 적외선수신모듈에 대한 전기회로가 정상적으로 연결되지 않았음을 인지하게 할 수 있다.
- [0061] 외부입출력단자(L6)는 적외선통신 모의해킹 실습장치(100)와 외부 컴퓨팅장치(200) 및 외부전원을 연결하는 구성요소로서, USB포트, HDMI 포트 및 외부전원소켓을 포함할 수 있다.
- [0062] 구체적으로 학습자가 적외선통신 모의해킹에 대한 소스코드를 작성하고 적외선통신 모의해킹에 따른 출력결과를 확인하기 위해서는 외부 컴퓨팅장치(200)와 연결될 필요가 있다. 외부입출력단자(L6)는 USB포트를 통해 외부 컴퓨팅장치(200)에서 작성된 소스코드를 수신할 수 있다.
- [0063] 바람직하게는 학습자는 외부입출력단자(L6)와 연결된 외부 컴퓨팅장치(200)에서 구동되는 프로그램을 통해 적외선통신 모의해킹에 대한 소스코드를 작성하고 적외선통신 모의해킹에 따른 출력결과를 확인할 수 있다.
- [0065] 또한, 외부입출력단자(L6)는 외부전원소켓을 통해 외부전원과 연결되어 적외선통신 모의해킹 실습장치(100)의 전원을 공급할 수 있다.
- [0067] 통신부(L4)는 외부에 존재하는 모의해킹 대상장치에 적외선 신호를 송신하는 구성요소이다. 상술한 바와 같이 학습자가 수행하는 공격시나리오에 따라 모의해킹 대상장치가 상이할 수 있다. 통신부(L4)는 별도의 적외선 송신장치를 더 포함하고, 모의해킹 대상장치가 TV, 스마트폰과 같이 외부 장치일 경우 해당 장치에 적외선 신호를 송신할 수 있다.
- [0068] 구체적으로 학습자가 적외선수신모듈 및 적외선송신모듈간의 송수신되는 데이터 패킷을 위변조하는 공격시나리오를 실습하는 경우, 학습자가 설계부(L1)에서 구성한 적외선수신모듈 및 적외선송신모듈이 모의해킹 대상장치가 되므로, 학습자는 본원 발명에서 제공하는 적외선통신 모의해킹 실습장치(100)만으로 적외선통신 모의해킹에 대한 출력결과를 확인할 수 있다.
- [0070] 한편, 학습자가 실습하고자 하는 공격시나리오가 'TV-리모콘간에 송수신되는 데이터 패킷을 해킹'하는 것에 해당하는 경우, 모의해킹 대상장치가 외부 장치인 TV가 될 수 있다. 상기와 같은 경우에 통신부(L4)는 적외선 신호를 생성하여 모의해킹 대상장치인 TV로 송신할 수 있다.
- [0071] 구체적으로 메인보드부(L2)는 통신부(L4)가 학습자가 설계부(L1)에서 구성한 적외선송신모듈이 생성하는 적외선 신호보다 증폭된 신호를 생성하도록 하여 외부 장치로 송신하도록 명령할 수 있다.
- [0072] 이와 같이 통신부(L4)를 구성하는 적외선송신장치는 실습과정에서 사용되는 적외선송신센서보다 성능이 우수한 소자를 사용하여 학습자가 구성한 적외선송신모듈보다 증폭된 신호를 외부 장치로 송신함으로써, 일반적인 교육 환경에서의 실습교육이 비교적 저렴한 소자로 수행되어 학습자가 구성한 적외선송신모듈이 외부장치로 적외선 신호를 송신하지 못하는 상황을 방지할 수 있다.
- [0073] 또한, 통신부(L4)의 적외선송신장치는 적외선통신 모의해킹 실습장치(100)의 전면부 일측에 배치하여, 외부 모의해킹 대상장치와 원활하게 적외선통신을 수행하게 함이 바람직하다.
- [0075] 신호분석부(L3)는 적외선수신모듈 및 적외선송신모듈 간에 송수신되는 데이터 패킷을 디스플레이하는 구성요소이다.
- [0076] 구체적으로 모의해킹을 시작함에 따라 적외선수신모듈 및 적외선송신모듈은 입력된 소스코드에 따라 적외선 통신을 수행하고, 신호분석부(L3)는 적외선 통신을 수행 중인 각 모듈 간에 송수신되는 데이터 패킷을 디스플레이

함으로써, 학습자가 적외선수신모듈 및 적외선송신모듈이 입력된 소스코드에 따라 정상적으로 동작하는 지 여부에 대한 정보를 제공할 수 있다.

[0078] 결과적으로 학습자는 설계부(L1)에서 적외선통신 모의해킹을 수행하는 적외선수신모듈 및 적외선송신모듈을 하드웨어적으로 구성해볼 수 있고, 외부입출력단자(L6)와 연결되는 외부 컴퓨팅장치(200)에서 상기 적외선수신모듈 및 적외선송신모듈에 대한 소스코드를 작성하여 입력하는 방식으로 소프트웨어적 실습을 수행할 수 있다.

[0079] 또한, 학습자가 구성한 적외선수신모듈 및 적외선송신모듈은 회로점검부(L5)에 의해 올바르게 구성되었는 지 여부가 점검될 수 있고, 신호분석부(L3)에 의해 적외선모의해킹이 수행됨에 따른 데이터 패킷이 디스플레이될 수 있다.

[0081] 결과적으로 학습자는 본원 발명에서 제공하는 적외선통신 모의해킹 실습장치(100)와 이와 연결되는 외부 컴퓨팅장치(200)만으로 적외선통신 모의해킹에 대한 하드웨어 및 소프트웨어적 실습교육을 수행할 수 있다.

[0083] 도 2는 본 발명의 일 실시예에 따른 외부 컴퓨팅장치(200)에 의해 적외선통신 모의해킹 실습장치(100)에 소스코드를 입력하는 단계를 도시한 것이다.

[0085] 도 2에 도시된 바와 같이, 적외선통신 모의해킹 실습장치(100)는 외부 컴퓨팅장치(200)와 연결되고, 학습자는 상기 외부 컴퓨팅장치(200)를 통해 적외선수신모듈 및 적외선송신모듈에 대한 소스코드를 작성하고 입력할 수 있다.

[0087] 구체적으로 본원 발명에서는 적외선수신모듈 또는 적외선송신모듈이 해킹공격을 수행하는 공격수행모듈이 될 수 있고, 학습자는 공격수행모듈이 되는 모듈에 적외선통신 해킹을 수행하는 소스코드인 공격코드를 입력하는 방식으로 적외선통신 모의해킹을 실습할 수 있다.

[0088] 또한, 학습자는 외부 컴퓨팅장치(200)를 통해 메인보드부(L2)를 동작시키기 위한 소스코드인 동작코드를 입력할 수도 있다.

[0090] 일례로, 학습자가 실습하고자 하는 공격시나리오가 '스니핑 시나리오'인 경우, 학습자는 적외선수신모듈에 데이터패킷을 스니핑하는 공격코드를 입력하고 적외선송신모듈 및 메인보드부(L2)에는 적외선통신을 수행하는 동작코드를 입력하는 방식으로 적외선통신 모의해킹을 수행하도록 할 수 있다.

[0092] 한편, 학습자단말이 적외선통신 모의해킹을 실습함에 따른 출력결과 또한 외부 컴퓨팅장치(200)에 디스플레이될 수 있다.

[0093] 구체적으로 학습자는 자신이 작성한 소스코드에 따라 적외선통신 모의해킹이 수행됨에 따른 출력결과를 확인함으로써, 자신이 구성한 적외선송신모듈 및 적외선수신모듈이 정상적으로 동작하는 지 여부를 확인할 수 있다.

[0095] 본 발명의 일 실시예에서 학습자가 실습하는 공격시나리오가 데이터 패킷을 스니핑하는 스니핑시나리오에 해당하는 경우, 외부 컴퓨팅장치(200)에는 적외선송수신모듈간에 송수신되는 데이터 패킷을 스니핑한 출력값이 디스플레이될 수 있다.

[0096] 또는 학습자가 실습하는 공격시나리오가 데이터 패킷을 위변조하는 위변조시나리오에 해당하는 경우, 외부 컴퓨팅장치(200)에는 공격수행모듈에 의해 위변조된 데이터패킷이 디스플레이될 수 있다.

[0098] 한편, 본 발명의 다른 실시예에서 학습자가 실습하는 공격시나리오가 'TV-리모콘'간의 동작을 제어하고자하는

공격시나리오인 경우, 모의해킹 대상장치인 TV의 동작여부가 적외선통신 모의해킹이 수행됨에 따른 출력결과일 수 있다.

[0099] 구체적으로 해당 공격시나리오에서 학습자는 공격수행모듈이 되는 적외선송신모듈을 구성하고, 상기 적외선송신 모듈에 TV의 전원을 ON-OFF하거나, 음량을 임의적으로 변경하는 공격코드를 입력할 수 있고, 해당 경우에 대한 적외선신호가 통신부(L4)에 의해 모의해킹 대상장치인 TV로 송신되어, 학습자가 작성한 공격코드에 따라 TV가 동작하는 지 여부를 확인할 수 있다.

[0101] 도 3은 본 발명의 일 실시예에 따른 통신부(L4)에 의해 모의해킹 대상장치에 적외선 신호를 송신하는 단계를 도시한 것이다.

[0103] 도 3에 도시된 바와 같이, 본원 발명의 적외선통신 모의해킹 실습장치(100)는 외부 모의해킹 대상장치와 적외선 통신을 수행할 수 있다. 상술한 바와 같이 본원 발명에서는 학습자가 실습하고자 하는 공격시나리오에 따라 모의해킹의 공격대상인 모의해킹 대상장치가 상이할 수 있고, 상기 모의해킹 대상장치가 TV, 스마트폰과 같이 외부 장치인 경우, 통신부(L4)를 통해 해당 장치에 적외선 신호를 송신할 수 있다.

[0105] 일례로 학습자가 적외선통신 모의해킹을 통해 TV의 동작을 제어하는 공격시나리오를 실습하는 경우, 학습자는 설계부(L1)상에서 적외선송신모듈을 하드웨어적으로 구성하고, 해당 적외선송신모듈에 대한 소스코드인 공격코드를 외부 컴퓨팅장치(200)에서 입력하는 방식으로 모의해킹을 실습할 수 있고, 메인보드부(L2)는 학습자가 작성한 공격코드에 대한 적외선신호, 즉 적외선송신모듈이 생성하는 적외선신호와 동일한 신호를 통신부(L4)가 생성하게 하여, 모의해킹 대상장치인 TV로 송신하게 할 수 있다.

[0107] 한편, 본 발명의 일 실시예에서는 2 이상의 학습자가 공동으로 적외선통신 모의해킹을 실습할 수 있다. 구체적으로 각 학습자는 각자의 적외선통신 모의해킹 실습장치(100)에서 적외선송신모듈 및 적외선수신모듈을 구성하고 이에 대한 소스코드를 작성할 수 있고, 적외선통신 모의해킹 실습장치(100) 서로간에 적외선통신을 수행하게 함으로써, 적외선통신 모의해킹이 정상적으로 동작하는 지 여부를 확인할 수 있다.

[0109] 도 4는 본 발명의 일 실시예에 따른 적외선통신 모의해킹 실습장치(100)를 활용하여 수행되는 IoT보안교육방법의 수행단계를 도시한 것이다.

[0111] 학습자는 적외선통신 모의해킹을 실습하고자 하는 공격시나리오를 선택(S1)하여 실습을 시작할 수 있다. 구체적으로 공격시나리오는 적외선통신 공격유형에 대한 다양한 공격사례가 구현된 시나리오이고, 학습자는 자신이 실습하고자 하는 공격시나리오를 선택하여 실습을 수행할 수 있다.

[0113] 이어서, 학습자는 설계부(L1)에서 전기회로를 구성(S2)할 수 있다. 구체적으로 학습자는 설계부(L1)의 브레드보드상에서 적외선송신센서, 적외선수신센서, 전원, 저항, 증폭기, 및 LED를 이용해 적외선송신모듈 및 적외선수신모듈을 구성하고, 상기 모듈들과 메인보드부(L2)를 전기적으로 연결하는 방식으로 적외선통신 모의해킹을 수행하는 전기회로를 설계할 수 있다.

[0115] 이어서, 학습자는 적외선송신모듈 및 적외선수신모듈에 대한 소스코드를 입력(S3)할 수 있다. 상술한 바와 같이 학습자가 선택한 공격시나리오에 따라 적외선송신모듈 또는 적외선수신모듈이 공격수행모듈이 될 수 있고, 학습자는 공격수행모듈에 적외선 모의해킹에 대한 공격코드를 입력하고, 공격수행모듈이 아닌 모듈 및 메인보드부(L2)에 적외선통신을 수행하는 동작코드를 입력할 수 있다.

[0116] 구체적으로 적외선송신모듈 또는 적외선수신모듈에 대한 소스코드는 외부입출력단자(L6)에 의해 연결된 외부 컴

퓨팅장치(200)에서 작성되어 입력될 수 있다.

- [0118] 결과적으로 S2단계를 수행하는 학습자는 설계부(L1)에서 적외선송신모듈 및 적외선수신모듈을 구성하고 이에 대한 전기회로를 설계하는 방식으로 적외선통신 모의해킹에 대한 하드웨어적 실습을 수행할 수 있고, S3단계를 수행하는 학습자는 외부입출력단자(L6)에 의해 연결된 외부 컴퓨팅장치(200)에서 소스코드를 입력하는 방식으로 적외선통신 모의해킹에 대한 소프트웨어적 실습을 수행할 수 있다.
- [0120] 이어서, 학습자는 입력한 소스코드를 컴파일(S4)할 수 있다. 구체적으로 학습자는 외부 컴퓨팅장치(200)에서 자신이 입력한 동작코드 및 공격코드를 디버깅하여 문법적, 논리적 오류가 없는지 점검하고, 정상입력된 소스코드를 컴파일하여 메인보드부(L2)에 입력할 수 있다.
- [0121] 한편, 상기 S4단계에서 학습자가 구성한 적외선송신모듈 및 적외선수신모듈이 전기적으로 올바르게 연결되었는지 여부를 점검할 수도 있다. 구체적으로 회로점검부(L5)는 적외선송신모듈 및 적외선수신모듈에 대한 전기회로의 단선 여부 또는 측정된 전압, 전류, 저항에 기초하여 적외선송신모듈 및 적외선수신모듈이 올바르게 구성되었는지를 점검할 수 있다.
- [0123] 한편, 상술한 바와 같이 적외선송신모듈 및 적외선수신모듈이 하드웨어적으로 올바르게 구성되지 않은 경우 회로점검부(L5)는 부저음을 출력하여 전기회로가 정상적으로 구성되지 않았음을 학습자가 인지하게 할 수 있다.
- [0125] 결과적으로 S4단계는 학습자가 구성한 적외선송신모듈 및 적외선수신모듈이 하드웨어 및 소프트웨어적으로 정상적으로 동작하는 지 점검하는 단계이다.
- [0127] 이어서, 학습자는 적외선송신모듈 및 적외선수신모듈을 동작시켜 적외선통신 모의해킹을 수행(S5 및 S6)하게 할 수 있다. 구체적으로 학습자는 상기 S4단계에서 점검이 완료된 적외선수신모듈 및 적외선송신모듈을 셋업하고 적외선통신 모의해킹을 수행하게 함으로써, 적외선송수신모듈이 정상적으로 동작하는 지 여부를 확인할 수 있다.
- [0129] 이어서, 본원 발명의 IoT보안교육방법에서는 적외선통신 모의해킹을 수행함에 따른 출력결과를 분석(S7)할 수 있다. 구체적으로 본원 발명에서는 적외선통신 모의해킹을 수행함에 따른 출력결과에 기초하여 공격코드가 유효한 지 여부를 판별하거나, 모의해킹 대상장치의 보안취약점을 분석할 수 있다.
- [0130] 상기 보안취약점이란 모의해킹 대상장치에서 소프트웨어 및 하드웨어적으로 발견되는 버그, 설계상 결함과 같은 약점을 의미하며, 더 구체적으로는 이러한 약점 가운데 공격(Exploit)당할 수 있는 결함을 의미하기도 한다.
- [0131] 결과적으로 본원 발명에서는 복수의 학습자에 의해 적외선통신을 활용한 전자제품(TV, 스마트폰 등)에 대한 모의해킹을 수행할 수 있고, 모의해킹 시뮬레이션 결과에 기초하여 공격대상이 되는 전자제품의 보안취약점을 발견하고, 해당 보안취약점을 개선하는 데 활용할 수 있다.
- [0133] 도 5는 본 발명의 일 실시예에 따른 적외선수신모듈 및 적외선송신모듈에 적외선통신 모의해킹을 수행하는 소스코드를 입력하고, 모의해킹 수행결과에 기초하여 모의해킹 대상장치에 대한 분석을 수행하는 단계를 도시한 것이다.
- [0135] 도 5의 (a) 및 (b)에 도시된 바와 같이, 본원 발명에서는 적외선통신 모의해킹을 실습할 수 있는 복수의 공격시나리오를 제공하고, 공격시나리오에 따라 공격수행모듈 및 모의해킹 대상장치가 상이할 수 있다.
- [0136] 구체적으로 스니핑시나리오의 경우, 도 5의 (a)에 도시된 바와 같이 적외선수신모듈이 공격수행모듈이 되고, 적

적외선송신모듈이 모의해킹 대상장치가 될 수 있다. 이와 같은 경우에 학습자는 메인보드부(L2) 및 적외선송신모듈에 적외선통신을 수행하는 동작코드를 입력하고, 적외선수신모듈에 데이터 패킷을 스니핑하는 공격코드를 입력하는 방식으로 모의해킹을 실습할 수 있다.

[0138] 또는 위변조시나리오의 경우, 도 5의 (b)에 도시된 바와 같이 적외선송신모듈이 공격수행모듈이 되고, 적외선수신모듈이 모의해킹 대상장치가 될 수 있다. 이와 같은 경우에 학습자는 메인보드부(L2) 및 적외선수신모듈에 적외선통신을 수행하는 동작코드를 입력하고, 적외선송신모듈에 데이터 패킷을 위변조하는 공격코드를 입력하는 방식으로 모의해킹을 실습할 수 있다.

[0140] 이와 같이 본원 발명에서는 학습자에게 적외선통신 모의해킹 사례에 대한 복수의 공격시나리오를 제공함으로써 학습자가 다양한 케이스로 적외선통신 모의해킹을 실습하게 할 수 있다.

[0142] 한편, 본원 발명에서 제공하는 공격시나리오는 교육자에 의해 추가된 추가공격시나리오를 더 포함할 수 있다. 상술한 바와 같이 공격시나리오는 적외선통신 공격사례가 재현된 시나리오일 수 있고, 교육자는 교육하고자 하는 공격사례에 따라 임의의 형태로 공격시나리오를 구성하여 추가할 수 있다.

[0143] 구체적으로 동일한 공격시나리오에 해당하더라도 사용되는 전자제품의 제품명, 및 제조사에 따라 입력해야 하는 동작코드 및 공격코드의 형태가 상이할 수 있고, 교육자는 실습하고자 하는 공격사례에 따라 추가공격시나리오를 구성 및 업로드하고, 학습자는 교육자에 의해 추가된 공격시나리오를 실습할 수 있다.

[0145] 한편 도 5의 (c)에 도시된 바와 같이, 본원 발명에서는 학습자가 실습한 적외선통신 모의해킹 실습결과에 기초하여 공격코드가 유효한 지 여부를 판별하거나, 공격대상이 되는 모듈의 보안취약점을 분석할 수 있다.

[0146] 상술한 바와 같이 본원 발명에서 제공하는 공격시나리오는 적외선통신 모의해킹에 대한 다양한 사례에 해당하고, 본원 발명에서는 학습자가 수행한 적외선통신 모의해킹 시뮬레이션 결과에 기초하여 공격코드가 유효한 지 여부를 판별하거나, 공격대상이 되는 모듈의 보안취약점을 분석할 수 있다.

[0147] 구체적으로 공격대상이 되는 모듈은 공격시나리오에 따라 TV, 스마트폰, 스마트TV와 같은 전자제품이 될 수 있고, 학습자가 수행한 적외선통신 모의해킹의 출력결과에 기초하여 해당 전자제품에 대한 보안취약점을 분석함으로써, 해당 전자제품에 대한 해킹공격을 방어하기 위한 대응수단을 개발하는 데 활용하게 할 수 있다.

[0149] 도 6은 본 발명의 일 실시예에 따른 학습자가 모의해킹을 수행함에 따른 스코어를 산출하는 단계를 도시한 것이다.

[0151] 도 6에 도시된 바와 같이, 상기 적외선통신 모의해킹 실습장치(100)를 활용하여 수행되는 IoT보안교육방법은, 상기 학습자가 적외선통신 모의해킹을 수행함에 따른 실습결과에 대한 스코어를 산출하는 스코어산출단계;를 더 포함하고, 상기 스코어산출단계는, 상기 회로점검부(L5)에 의해 점검된, 상기 학습자가 구성한 적외선수신모듈, 및 적외선송신모듈이 전기회로적으로 올바르게 구성되었는 지 여부에 대한 스코어를 산출하는 제1스코어산출단계; 상기 학습자가 작성한 적외선수신모듈, 및 적외선송신모듈을 동작시키는 소스코드에 대한 디버깅을 수행하여, 상기 소스코드의 유효성에 기초하여 스코어를 산출하는 제2스코어산출단계; 및 상기 학습자가 입력한 상기 소스코드와 모의해킹이 수행됨에 따라 출력된 출력결과를 비교하여, 모의해킹이 정상적으로 수행되는지 여부에 기초하여 스코어를 산출하는 제3스코어산출단계;를 포함할 수 있다.

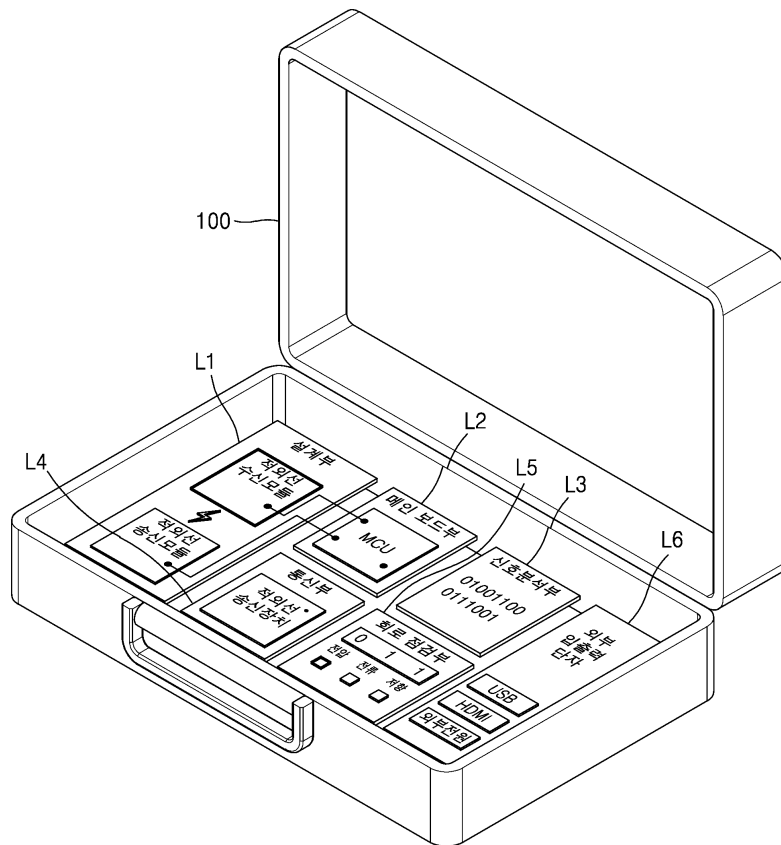
[0153] 상술한 바와 같이 학습자는 본원 발명에서 제공하는 적외선통신 모의해킹 실습장치(100) 및 이와 연결된 외부 컴퓨팅장치(200)를 통해 적외선통신 모의해킹을 실습할 수 있다. 본원 발명에서는 적외선통신 모의해킹 실습수행과정 및 실습결과에 기초하여 학습자에 대한 스코어를 산출하여 학습자에게 제공할 수 있다.

- [0155] 구체적으로 학습자는 도 6에 도시된 순서에 따라 적외선통신 모의해킹을 실습할 수 있고, 본원 발명에서는 S2단계에서 학습자가 구성한 적외선수신모듈 및 적외선송신모듈이 전기적으로 올바르게 연결되었는 지 여부에 기초하여 제1스코어(10)를 산출하고, S3단계에서 적외선수신모듈 및 적외선송신모듈에 입력된 소스코드(공격코드 및 동작코드)의 유효성에 기초하여 제2스코어(20)를 산출하고, S7단계에서 적외선통신 모의해킹이 수행됨에 따라 출력된 출력결과에 기초하여 제3스코어(30)를 산출할 수 있다.
- [0156] 결과적으로 본원 발명에서는 학습자의 실습수행과정 및 모의해킹 결과에 대한 스코어를 산출하여 학습자에 제공할 수 있다.
- [0158] 도 7은 본 발명의 일 실시예에 따른 교육자단말 및 1 이상의 학습자단말에 의해 IoT보안교육이 실시되는 일 모습을 도시한 것이다.
- [0160] 도 7에 도시된 바와 같이, 본원 발명에서 제공하는 적외선통신 모의해킹 실습장치(100)를 활용하여 수행되는 IoT보안교육방법은 동일한 실습교육을 수강하는 1 이상의 학습자 및 상기 학습자의 실습교육을 진행하고 관리감독하는 교육자에 의해 수행될 수 있다.
- [0161] 구체적으로 도 7은 본원 발명의 적외선통신 모의해킹 실습장치(100)를 활용하여 수행되는 IoT보안교육방법이 수행되는 일 모습으로서, 교육자는 복수의 학습자단말(2.1, 2.2, 2.3, 2.4, 2.5, 및 2.6)에 대한 실습수행과정 및 실습결과에 대한 정보, 더 구체적으로는 각 학습자가 기록한 스코어를 제공할 수 있다.
- [0163] 또한, 본원 발명에서는 각 학습자의 실습수행과정 및 실습결과에 대한 스코어가 산출되므로, 교육자는 학습수행능력이 떨어지는 학습자, 구체적으로 스코어가 낮은 학습자에 실습교육에 대한 답안을 제공할 수 있다. 구체적으로 학습자(2.6)은 타 학습자에 비해 학습수행능력이 떨어져 낮은 스코어를 기록한 학습자로서, 교육자는 상기와 같이 학습수행능력이 떨어지는 학습자(2.6)에 답안(3)을 제공할 수 있다.
- [0164] 구체적으로 상기 답안(3)은 학습자(2.6)가 소스코드를 입력하고 출력결과를 확인할 수 있는 컴퓨팅장치를 통해 제공될 수 있다.
- [0166] 상기와 같이 본원 발명에서는 적외선통신 모의해킹 실습교육을 수행하는 복수의 학습자 개개인인의 학습수행능력에 대한 스코어를 산출함으로써, 교육자가 복수의 학습자들의 교육과정을 체계적으로 관리하도록 할 수 있다.
- [0168] 본 발명의 일 실시예에 따르면 학습자는 적외선통신 공격유형에 대한 복수의 공격시나리오 중 실습하고자 하는 공격시나리오를 선택하여, 적외선통신 모의해킹을 실습할 수 있다.
- [0169] 본 발명의 일 실시예에 따르면 학습자는 적외선통신 모의해킹을 수행하는 적외선해킹모듈을 디자인하고 전기회로를 구성해보는 방식으로 적외선통신 모의해킹을 실습할 수 있다.
- [0170] 본 발명의 일 실시예에 따르면 학습자는 적외선통신 모의해킹을 수행하는 적외선해킹모듈에 대한 소스코드를 작성하는 방식으로 적외선통신 모의해킹을 실습할 수 있다.
- [0171] 본 발명의 일 실시예에 따르면 학습자가 구성한 적외선해킹모듈이 적외선통신 모의해킹을 수행한데 따른 출력결과를 제공할 수 있다.
- [0172] 본 발명의 일 실시예에 따르면 학습자가 구성한 적외선통신 모의해킹 수행과정 및 수행결과에 따른 스코어를 산출하여 제공할 수 있다.
- [0173] 본 발명의 일 실시예에 따르면 다수의 학습자를 관리감독하는 교육자에게 학습자 개개인의 실습진행정보 및 스코어를 제공할 수 있다.

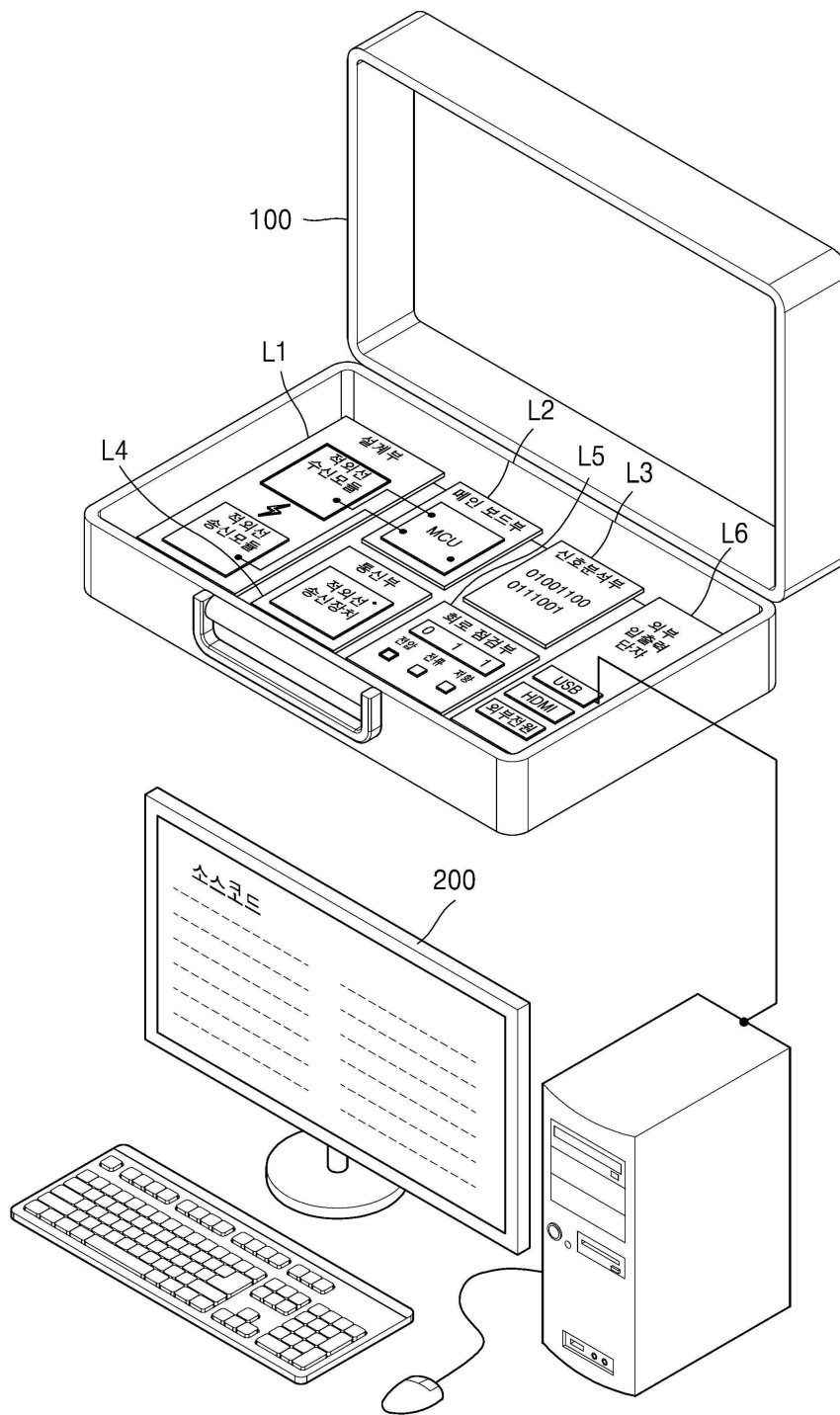
[0175] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

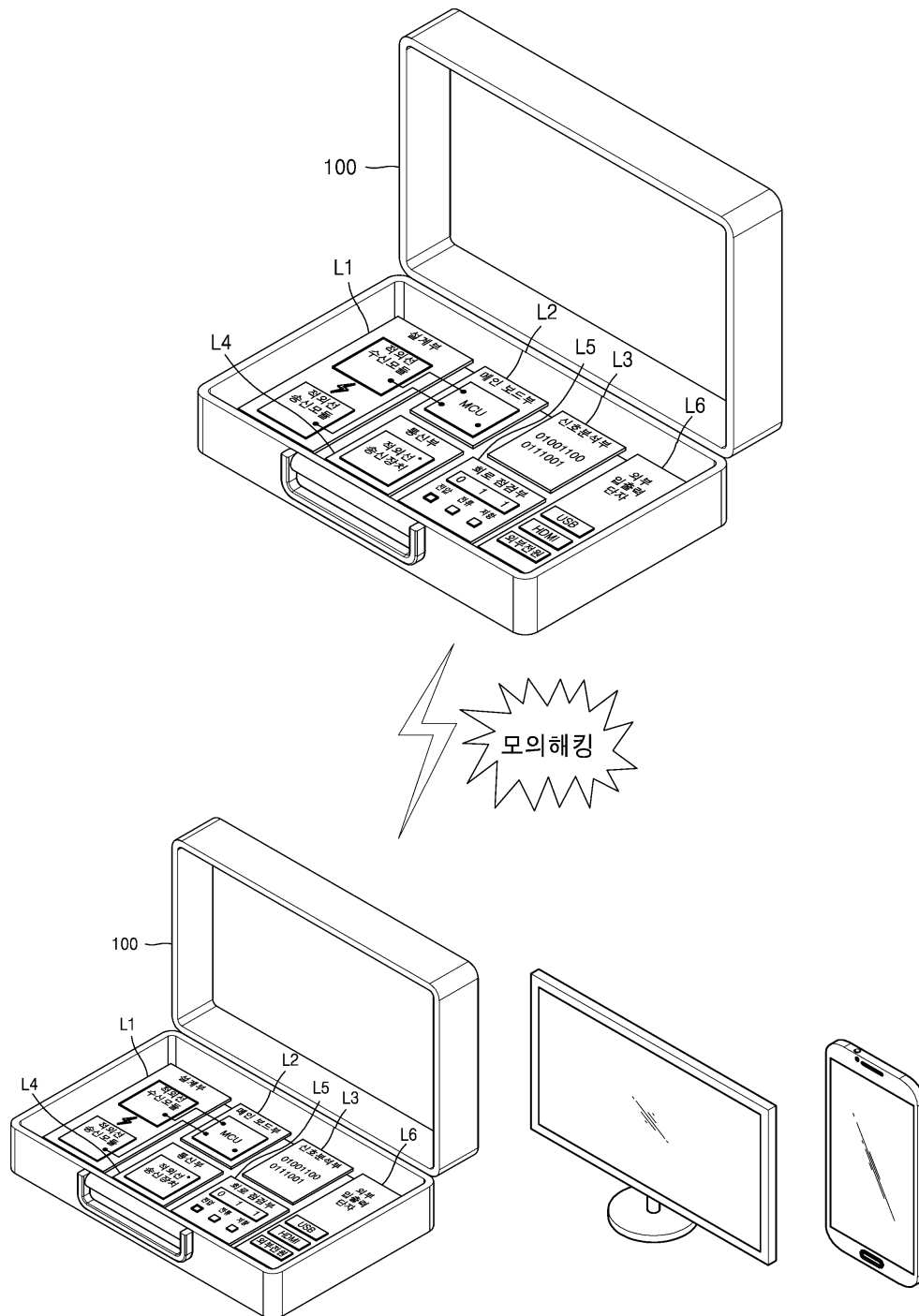
도면1



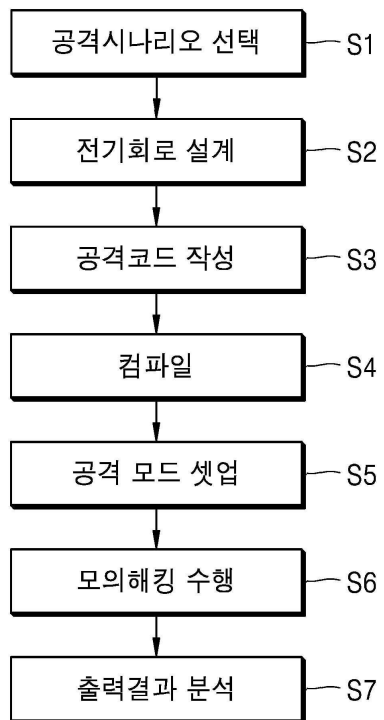
도면2



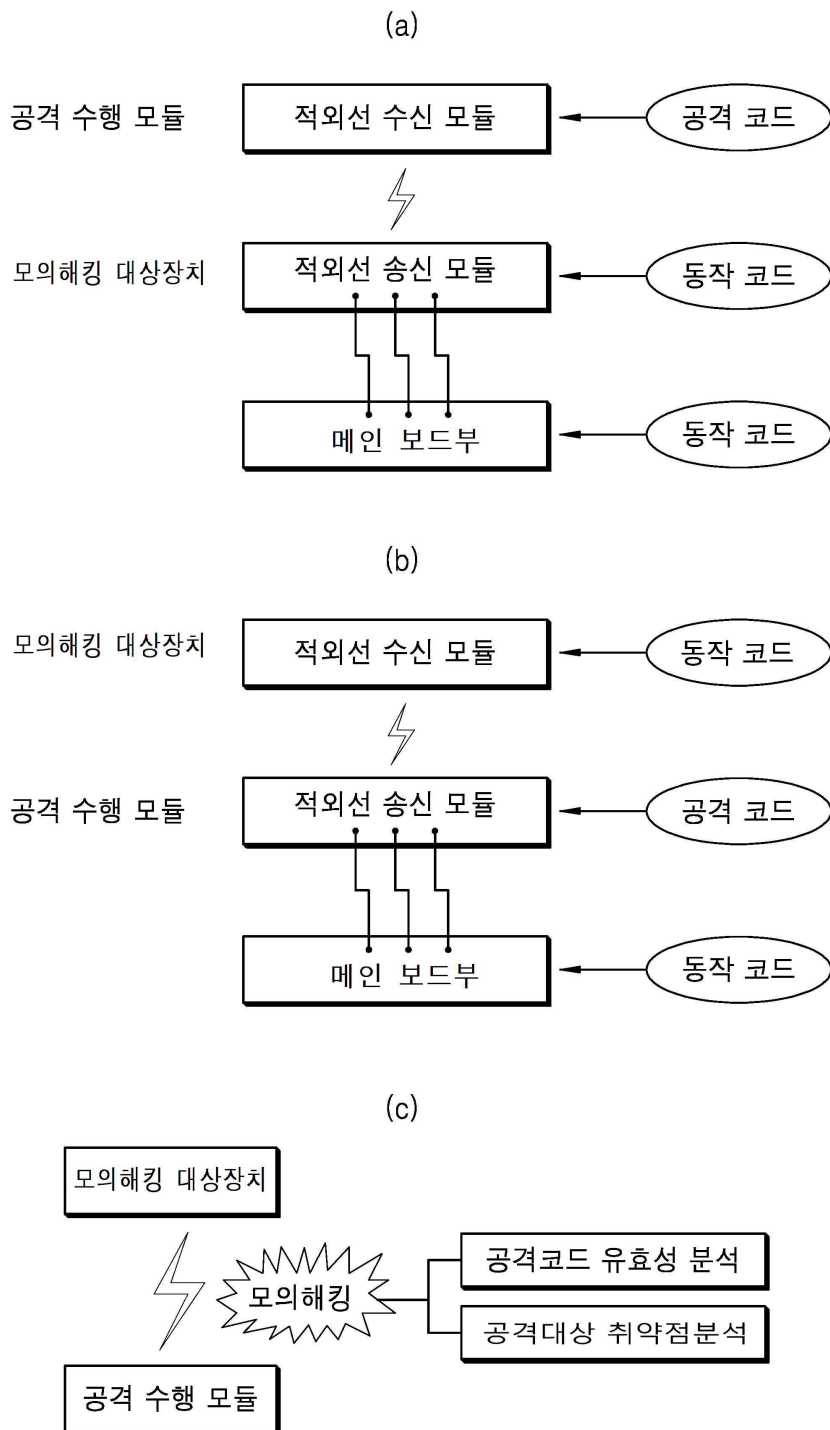
도면3



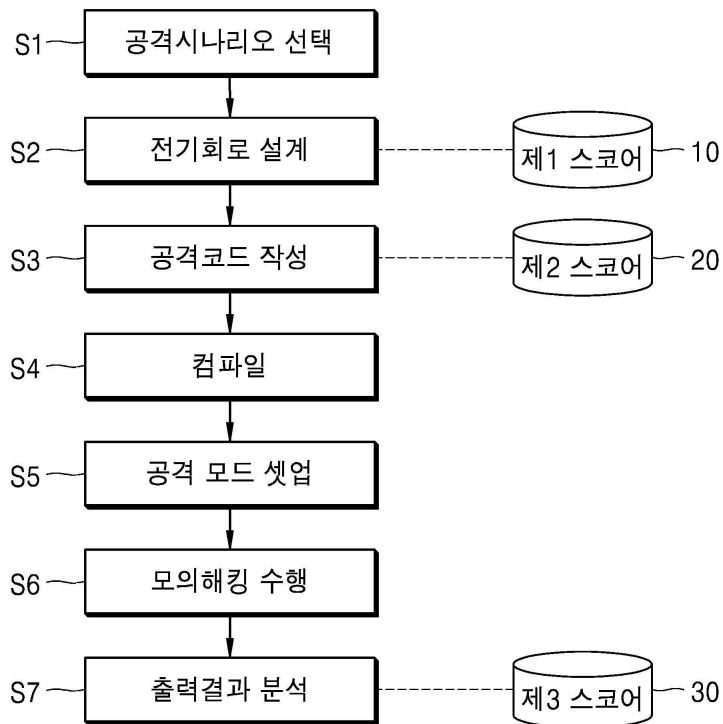
도면4



도면5



도면6



도면7

